(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/33936 A3

(51) International Patent Classification[7]: G06F 17/60, 1/00

(21) International Application Number: PCT/US00/41623

(22) International Filing Date: 26 October 2000 (26.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/430,331 29 October 1999 (29.10.1999) US

(71) Applicant: PRIVACOMP, INC. [US/US]; 2450 Central Avenue, Suite D, Boulder, Colorado 80301 (US).

(72) Inventor: KNAPP, Terry; 7451 North 63rd Street, Longmont, CO 80503 (US).

(74) Agents: GRAZIANO, James, M. et al.; Patton Boggs LLP, P.O. Box 270930, Louisville, CO 80027 (US).

(81) Designated States *(national)*: AU, BR, CA, MX.

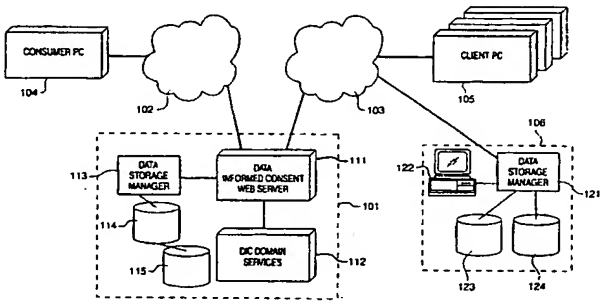
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *with international search report*

(88) Date of publication of the international search report:
13 December 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR PROVIDING DYNAMIC DATA INFORMED CONSENT TO PROVIDE DATA PRIVACY AND SECURITY IN DATABASE SYSTEMS AND IN NETWORKED COMMUNICATIONS



(57) Abstract: The Dynamic Data Informed Consent system enables consumers to govern the flow of their personal data regardless of the nature of the information. The Dynamic Data Informed Consent system creates a means by which Data Informed Consent obtained from a consumer can govern a transaction environment for the exchange of consumer (e.g. health care) information by and among client organizations (e.g. health care businesses). The further objective of the Dynamic Data Informed Consent system is to provide the data access transaction environment (including Data Informed Consent) in its entirely, in order to reduce its client businesses' development and administrative costs, and to assure compliance with legal requirements for data exchange re: security, privacy and confidentiality. The Dynamic Data Informed Consent System educates (informs) theconsumer regarding the consumer's rights to privacy, security and confidentiality of personal information and the general and specific obligations of parties that may be authorized by the consumer to use the consumer's information. The Dynamic Data Informed Consent system enables consumers to govern the flow of their personal data regardless of the nature of the information. The consumer can define a set of data access rules which designate the client companies who have access to the consumer's personal data and the particular segments of that personal data to which each client company is entitled. The Data Informed Consent is dynamic in that the consumer can use their Digital Certificate at any time to access and modify their Data Informed Consent provided to the Dynamic Data Informed Consent system.

WO 01/33936 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41623

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 01834 A (COUEIGNOUX PHILIPPE J M) 14 January 1999 (1999-01-14) page 3, line 4 -page 5, line 13 page 19, line 14 - line 28 page 26, line 4 - line 25	1-4,6,9, 12-14, 18-21, 23,26, 29,31
Y		5,7,10, 11,15, 16,22, 24,27, 28,32,33
A	abstract	30

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 2001	06/08/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41623

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 835 087 A (EISNER JASON M ET AL) 10 November 1998 (1998-11-10) column 45, line 36 -column 48, line 26	5,7,15, 16,22, 24,32,33
Y	US 5 339 403 A (PARKER THOMAS A) 16 August 1994 (1994-08-16) column 2, line 9 - line 23	10,27
P,Y	EP 0 991 005 A (NCR INT INC) 5 April 2000 (2000-04-05) abstract column 7, line 9 - line 19 column 13, line 44 -column 14, line 26	11,28
A	US 5 918 014 A (ROBINSON GARY B) 29 June 1999 (1999-06-29) column 6, line 52 -column 7, line 14	3-5,7, 20-22,24

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/41623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9901834 A	14-01-1999	US 6092197 A	18-07-2000
		EP 1008084 A	14-06-2000
US 5835087 A	10-11-1998	US 5758257 A	26-05-1998
		AU 703247 B	25-03-1999
		AU 4410396 A	19-06-1996
		CA 2207868 A	06-06-1996
		EP 0796538 A	24-09-1997
		US 6020883 A	01-02-2000
		WO 9617467 A	06-06-1996
		US 5734720 A	31-03-1998
		US 5754938 A	19-05-1998
		US 5754939 A	19-05-1998
		US 6088722 A	11-07-2000
		US 6029195 A	22-02-2000
US 5339403 A	16-08-1994	AU 634653 B	25-02-1993
		AU 7620991 A	14-11-1991
		DE 69130461 D	17-12-1998
		DE 69130461 T	10-06-1999
		EP 0456386 A	13-11-1991
		ZA 9103322 A	26-02-1992
EP 0991005 A	05-04-2000	US 6253203 B	26-06-2001
		JP 2000293421 A	20-10-2000
US 5918014 A	29-06-1999	AU 1566597 A	11-08-1997
		WO 9726729 A	24-07-1997

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/33936 A2

(51) International Patent Classification: Not classified

(21) International Application Number: PCT/US00/41623

(22) International Filing Date: 26 October 2000 (26.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/430,331 29 October 1999 (29.10.1999) US

(71) Applicant: PRIVACOMP, INC. [US/US]; 7451 North 63rd Street, Longmont, CO 80503 (US).

(72) Inventor: KNAPP, Terry; 7451 North 63rd Street, Longmont, CO 80503 (US).

(74) Agents: GRAZIANO, James, M. et al.; Duft, Graziano & Forest, P.C., P.O. Box 270930, Louisville, CO 80027 (US).

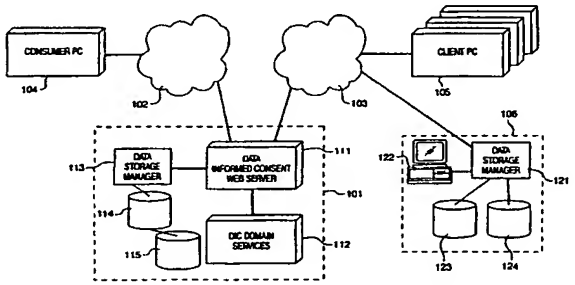
(81) Designated States *(national)*: AU, BR, CA, MX.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR PROVIDING DYNAMIC DATA INFORMED CONSENT TO PROVIDE DATA PRIVACY AND SECURITY IN DATABASE SYSTEMS AND IN NETWORKED COMMUNICATIONS



(57) Abstract: The Dynamic Data Informed Consent system enables consumers to govern the flow of their personal data regardless of the nature of the information. The Dynamic Data Informed Consent system creates a means by which Data Informed Consent obtained from a consumer can govern a transaction environment for the exchange of consumer (e.g. health care) information by and among client organizations (e.g. health care businesses). The further objective of the Dynamic Data Informed Consent system is to provide the data access transaction environment (including Data Informed Consent) in its entirely, in order to reduce its client businesses' development and administrative costs, and to assure compliance with legal requirements for data exchange re: security, privacy and confidentiality. The Dynamic Data Informed Consent System educates (informs) theconsumer regarding the consumer's rights to privacy, security and confidentiality of personal information and the general and specific obligations of parties that may be authorized by the consumer to use the consumer's information. The Dynamic Data Informed Consent system enables consumers to govern the flow of their personal data regardless of the nature of the information. The consumer can define a set of data access rules which designate the client companies who have access to the consumer's personal data and the particular segments of that personal data to which each client company is entitled. The Data Informed Consent is dynamic in that the consumer can use their Digital Certificate at any time to access and modify their Data Informed Consent provided to the Dynamic Data Informed Consent system.

WO 01/33936 A2

SYSTEM FOR PROVIDING DYNAMIC DATA INFORMED CONSENT TO PROVIDE DATA PRIVACY AND SECURITY IN DATABASE SYSTEMS AND IN NETWORKED COMMUNICATIONS

Field of the Invention

This system relates to the fields of database management systems and networked electronic communications and, in particular, to a system for managing the authorization of parties to access data contained in databases and transmitted in a networked environment.

Problem

It is a problem in the field of modern electronic data interchange among parties operating in networked environments (especially using the open medium of the Internet) and using large databases to ensure the privacy of personalized data that is stored and exchanged among parties unrelated to the owner (subject) of the information. In many database management systems, there are a number of classes of users who require access to data stored in the database system, but these classes of users should have authorization to access only a predefined portion of the data contained therein. Furthermore, there is a need for non-uniformity of access that may be authorized across a particular class of users. The consumer whose data is stored in the database should have the capability to selectively authorize specific users in a class to access the consumer's data. Likewise, the consumer should have the ability to authorize the conditions under which the consumer's personal data is exchanged among third parties. Existing database management systems fail to provide a consumer who has data stored in the database system the ability to participate in the management of the authorization of parties to access the consumer's data contained in the database, or to grant transaction authorization among parties using the consumer's data. The typical data access management paradigm is to require the consumer to provide blanket data access and transaction authorization to broad classes of users, without the consumer having the ability to define the authorization to a finer degree of granularity, or being able to revoke authorization to access the consumer's data in a simple manner.

In the more general field of consumer personal data, public concerns are escalating over the management of consumer personal information, such as

individualized health care information, and especially information stored in electronic format. The issue has reached a level of significance such that U.S. Congress has moved to address these concerns, spurred by numerous consumer rights and privacy groups. As an example of the response to these concerns, Section 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) required that the Secretary of Health and Human Services issue recommendations to Congress regarding regulatory protection of privacy, confidentiality and consumer access to individually identifiable health information. However, there is presently no viable technology-based system for satisfying these above-listed needs in the field of health information or any other field that uses consumer personal data.

For those engaged in healthcare operations - payers, providers and care plans - the need to comply with the aforementioned Health and Human Services regulations imposes significant new burdens of expense and liability relative to the management of health care information. The proposed regulations force health care businesses that transact, hold or distribute personalized health care data for treatment, payment, research, or other purposes to each obtain the consent of each consumer (patient) who may be the subject of such data. The consent must be informed - i.e., the consumer must know what information is to be used, for what purposes, with whom it is to be shared, etc. Furthermore, each health care business must manage the consumer's informed consent to comply with the wishes of the consumer regarding disclosure of the data. Each health care business must maintain a log and an audit trail of disclosures, with the log containing time and date stamp data, assuring that the disclosure is authorized, that the purpose for which the data is disclosed is authorized, and that the minimum data set to serve the intended purpose is disclosed. The audit trail must be maintained for the life of the record and must be made available to the consumer on request. Failure of the business to manage consumer personalized health care data as described in the proposed regulations subjects the business to official sanctions and penalties, and to liability and legal action for redress.

Attempts by health care businesses to meet privacy, confidentiality and consumer access statutes and regulations require significant development and administrative expenses, and entail risk and attendant liability. However, regardless of the extent to which any health care business unilaterally attempts compliance, there

is no certainty of such compliance. The reason is that the nature of the proposed regulations requires that the transactions involving health care data be in compliance. Therefore, in most cases (billing, exchange of clinical data, etc.) transactions involve two independent businesses. One business may be compliant, the other, not compliant, thus creating transaction non-compliance for both businesses. Even within a large organization, it may not be appropriate that certain workers have access to consumer files, thus creating a violation unless a suitable privacy mechanism is in place.

The regulations for mandated consumer control of the flow of personal health care data are expected to be propagated into other sectors of industry that currently manage, store and distribute consumer personal information. Thus, the issues faced by the health care industry are expected to be the same issues faced in other industries that gather, store, and provide access to consumer personal information – such as the banking, credit, legal, retail sales and accounting fields.

There are six recognized conditions of privacy that any technology-based system must accommodate:

Notice - The individual has the right to know that there is the possibility of collection of personally identifiable data (PII).

Choice - The individual has the right to choose not to have the data collected.

Use - The individual has the right to know how data is expected to be used and to restrict its use.

Security - The individual has the right to know the extent to which the data is protected.

Correction - The individual has the right to challenge the accuracy of the data and to provide corrected information.

Enforcement - The individual has the right to seek legal relief through appropriate channels to protect privacy rights.

A technology-based solution to ensure privacy and confidentiality for individually identifiable electronic information must take into account all six conditions, and thereby must reveal the conditions upon which disclosure is authorized and allow for changes in authorization over time, hence the concept of dynamic data informed consent.

Solution

The above described problems are solved and a technical advance achieved by the present system for providing dynamic data informed consent which enables consumers to govern the flow of their personal data regardless of the nature of the information. The goal of the Dynamic Data Informed Consent system is to create a mechanism by which Data Informed Consent obtained from a consumer can govern a transaction environment for the exchange of consumer (e.g. health care, financial, and the like) information by and among client organizations (e.g. health care businesses, banks and credit bureaus, and the like). The further objective of the Dynamic Data Informed Consent system is to provide the data access transaction environment (including Data Informed Consent) in its entirely, in order to reduce its client businesses' development and administrative costs, and to assure compliance with legal requirements for data exchange re: privacy and confidentiality.

Various means of securing the data are available, such as symmetric and asymmetric encryption key systems and protected lists. Various means of authentication of users are available, including digital signatures, passwords, biometrics and smart cards. In the present embodiment, the security of data is addressed through the means of a public key infrastructure and digital certificate issuance to authorized and authenticated users. Each transaction participant consists of a client company that holds a general Digital Certificate to authenticate that company, as well as sub-Digital Certificates for various classes of authorized workers employed by that company. Each Digital Certificate bears a unique identifier to ensure that it can be tracked. (Other means of authentication, such as smart cards or biometric reading devices, may also be used for authentication of authorized parties.) Each Digital Certificate issued to client companies is accompanied by a set of requirements governing its use that are designed for compliance with regulations and the data access limitations defined by the consumer. Each client company specifically attests to its compliance with those stipulations. Each consumer is authenticated and issued a Digital Certificate or other means of authentication to use in the generation of a Dynamic Data Informed Consent and for use in the event of electronic changes to the Data Informed Consent in the course of the Dynamic Data Informed Consent system's service as agent for the consumer. Thus, the consumer

can define a set of data access rules which designate the client companies, and classes of employees within those companies, who have access to the consumer's personal data (termed "proprietary consumer specific data" herein) and the particular segments of that proprietary consumer specific data to which each client company is entitled. The Data Informed Consent is dynamic in that the consumer can use their Digital Certificate (or other authenticated means) at any time to access and modify their Data Informed Consent provided to the Dynamic Data Informed Consent system.

The medium for data transmission among the parties served by the Dynamic Data Informed Consent system is any electronic data communication system, such as: the Internet, Intranet, Virtual Private Network (VPN), Wide Area Network, Public Telephone Switched Network (PTSN), and the like. The data transmitted by transacting parties need never be seen, except for the minimum data necessary to assure identity of the subject, nor held by the Dynamic Data Informed Consent system. The Dynamic Data Informed Consent system acts as a compliance clearinghouse for the data flow (i.e., as traffic cop, not as custodian). In providing compliance assurance, the Dynamic Data Informed Consent system maintains for each Data Informed Consent a log of users, category of proprietary consumer specific data, purpose for which the proprietary consumer specific data is used, which log is time and date stamped. The Dynamic Data Informed Consent System maintains the audit trail of all uses of proprietary consumer specific data, together with audit analysis software to determine if any breach of the System's authorization structure occurs. The components of the Dynamic Data Informed Consent system by which dynamic Data Informed Consent modulates a security structure for the transmission and exchange of personal electronic data include:

A public key infrastructure (PKI) that provides robust encryption of all proprietary consumer specific data routed through the Dynamic Data Informed Consent system. Encryption modalities other than PKI may be employed to implement this function.

Digital certificates to provide ongoing authentication of approved parties, and associated constraints on use and attestations provided by the parties to whom they are issued. Other means of authentication such as passwords,

biometrics and smart cards may be used to implement this function.

A data center and service center managed by a controlling entity to manage both the issuance of digital certificates to participants (client companies and consumers), and the management of Data Informed Consent.

The Data Informed Consent module and methods of management as a governor of the transaction environment. The Data Informed Consent module consists of a rules-driven (inference engine-driven) database management system (DBMS) with lookup tables corresponding with the authorizations, or revocations thereof, placed by each consumer executing Data Informed Consent.

The Data Informed Consent module itself consists of the following essential elements:

A cross-platform compatible, scalable data base management system (DBMS) such as Oracle or Sybase.

A graphic user interface to allow consumer interaction with the Dynamic Data Informed Consent system.

A forms-driven component for the consumer to understand their legal rights and to modify authorizations for various consumer-specified entities to hold, access and transact with (disclose) the consumer's proprietary consumer specific data.

A component to enable the consumer to change the level of authorization to and among authorized parties.

A component to enable the consumer to segmentalize (compartmentalize) proprietary consumer specific data.

Look-up tables with reference to individual consumers that list authorizations and similar tables that consist of revocations of authorizations.

A component to log all instances of authorized use of proprietary consumer specific data and unauthorized attempts to use proprietary consumer specific data.

A component to audit and analyze the logs that catalogue authorized and attempts at unauthorized use of proprietary consumer specific data.

Software interface with PKI or another data security platform, such that

consumer identifiers are accessed and checked against authorization and authorization revocation lists.

Thus, the Dynamic Data Informed Consent system enables consumers to govern the flow of their proprietary consumer specific data regardless of the nature of the information. The consumer can define a set of data access rules which designate the client companies who have access to the consumer's proprietary consumer specific data and the particular segments of that proprietary consumer specific data to which each client company is entitled. The Data Informed Consent is dynamic in that the consumer can use their Digital Certificate at any time to access and modify their Data Informed Consent provided to the Dynamic Data Informed Consent system.

Brief Description of the Drawing

Figure 1 illustrates in block diagram form the overall architecture of the Dynamic Data Informed Consent system and a typical environment in which it is operational;

Figure 2 illustrates additional details of the Dynamic Data Informed Consent system and provides an indication of a typical data flow therein;

Figures 3 and 4 illustrate in flow diagram form the operation of the Dynamic Data Informed Consent system of Figure 2 in processing a typical transaction;

Figure 5 illustrates in block diagram form the structure of the Dynamic Data Informed Consent Domain;

Figure 6 illustrates the communication pathways that are used in the processing of an institution query to an information management system IMS, using the Dynamic Data Informed Consent system as an authorizing agency to enable the institution to access a consumer's proprietary consumer specific data; and

Figure 7 illustrates in flow diagram form the operation of this information management system IMS, using the Dynamic Data Informed Consent system as an authorizing agency to enable the institution to access a consumer's proprietary consumer specific data.

Detailed Description

The Dynamic Data Informed Consent system enables consumers to govern the flow of their proprietary consumer specific data regardless of the nature of the

proprietary consumer specific data. The goal of the Dynamic Data Informed Consent system is to create a mechanism by which Data Informed Consent can govern a transaction environment for the exchange of consumer (e.g. health care, financial, and the like) information by and among client organizations (e.g. health care businesses, financial institutions, and the like). The further objective of the Dynamic Data Informed Consent system is to provide the transaction environment (including Data Informed Consent) in its entirely, in order to reduce its client businesses' development and administrative costs, and to assure compliance with legal requirements for exchange of proprietary consumer specific data re: privacy and confidentiality.

Figure 1 shows in block diagram form the overall architecture of the Dynamic Data Informed Consent system 101 and a typical environment in which it is operational. The Dynamic Data Informed Consent system 101 is interconnected via a data transmission medium 102 (such as the Public Telephone Switched Network) to a consumer's terminal device 104, such as a personal computer, and via a data transmission medium 103 (such as the Internet) to a client's terminal device 105, such as a personal computer. The Dynamic Data Informed Consent system 101 itself comprises an interface element 111, such as a WEB server, to interconnect the Dynamic Data Informed Consent system 101 with the respective data transmission medium 102, 103, thereby enabling both the consumer and clients to interconnect with the Dynamic Data Informed Consent system 101. The Dynamic Data Informed Consent system 101 also includes a Data Informed Consent domain module 112 as is described in additional detail below. The Dynamic Data Informed Consent system 101 can optionally include a data storage manager 113 and its associated data storage devices 114, 115 which store the proprietary consumer specific data, or, alternatively, the proprietary consumer specific data can be stored in whole or in part in one or more external data storage system(s) 106. The external data storage system 106 includes a data storage manager 121, administrator interface terminal 122 and its associated data storage devices 123, 124, which stores the proprietary consumer specific data. The Dynamic Data Informed Consent system 101 functions to provide a data access transaction environment for proprietary consumer specific data, including but not limited to the typical steps of: receiving requests for proprietary consumer specific data from clients, authentication of clients, maintaining security of

the proprietary consumer specific data, issuance of digital certificates to authorized and authenticated users to enable clients to access the proprietary consumer specific data, under the terms and conditions specified by the consumer.

Definitions:

Confidentiality - This comprises a secret communication with another party (trusted other). The confidential exchange of information implies that the information is exchanged or shared with the trusted other who is trusted to keep the information secret, i.e. the trusted other will not disclose the information to others.

Privacy - This comprises the state of being free from unsanctioned intrusion. Privacy is often confused with security. Security implies safety from intrusion, while privacy invokes the ability of a person to avoid intrusion unless that person authorizes the intrusion.

Security - This comprises the level to which data is safe from unauthorized use. Security requires mechanisms which protect the data from unauthorized use. The dynamic process of authorization or revocation of authorization via operation of a security mechanism is the exercise of privacy.

Data Informed Consent - The process by which a consumer is informed about their rights under the law, and the responsibilities of parties who use their personalized information ("General Advisory"), as well as the manner in which their data is used, managed and protected ("Specific Advisory"). This process provides for interactive consumer control of disclosure authorization and the revocation thereof ("Dynamic Consent"). In other words Data Informed Consent dictates what client companies can do with the consumer's data - hence a two-way interaction: The present system informs the consumer of the various options; consumers consent to client companies accessing their data via the present system pursuant to the parameters specified by the consumer.

Health Care Example

The description that follows pertains to the current challenge of managing security and privacy for health care information. While the example is focused on the use of electronic apparatus to implement the data storage, data exchange, data security, and privacy components of the Dynamic Data Informed Consent system, it is expected that portions of this Dynamic Data Informed Consent system may entail

the use of traditional paper-based forms and processes. The present example is used due to its pertinence to the present needs of the health care industry and is intended to be illustrative of the concepts embodied in the Dynamic Data Informed Consent system and is not intended to limit the scope of the Dynamic Data Informed Consent system as embodied in the claims appended hereto. The concepts illustrated herein are directly applicable to numerous other Dynamic Data Informed Consent applications, including but not limited to: banking, credit agencies, employment, education, taxing agencies, government and their regulatory agencies, and the like.

For those engaged in healthcare operations - payers, providers and care plans - the need to comply with the aforementioned Health and Human Services regulations imposes significant new burdens of expense and liability relative to the management of health care information. The proposed regulations force health care businesses that transact, hold or distribute personalized health care data for treatment, payment, research, or other purposes to each obtain the consent of each consumer (patient) who may be the subject of such data. The consent must be informed - i.e., the consumer must know what information is to be used, for what purposes, with whom it is to be shared, etc. Furthermore, each health care business must manage the consumer's informed consent to comply with the wishes of the consumer regarding disclosure of the proprietary consumer specific data. Each health care business must maintain a log and an audit trail of disclosures, with the log containing time and date stamp data, assuring that the disclosure of the proprietary consumer specific data is authorized, that the purpose for which the proprietary consumer specific data is disclosed is authorized, and that the minimum data set to serve the intended purpose is disclosed. The audit trail must be maintained for the life of the record and must be made available to the consumer on request. Failure of the business to manage consumer personalized health care data as described in the regulations subjects the business to official sanctions and penalties, and to liability and legal action for redress.

Dynamic Data Informed Consent

The Dynamic Data Informed Consent system interactively manages the wishes of the consumer regarding all elements of disclosure of proprietary consumer specific

data (personalized electronic health care data). The management of Data Informed Consent pertaining to paper-based records is a manual administrative process designed to reflect the principles embodied in dynamic, electronic Data Informed Consent management system described herein.

The general provisions that the Dynamic Data Informed Consent system must accommodate in deploying Data Informed Consent typically include the following:

1.) There is a duty not to use or disclose health information except as authorized by the consumer, or as explicitly permitted by legislation or regulations.

2.) Clients (providers or payers) are permitted to use the health information only for purposes compatible with and directly related to the purposes for which the information was collected or received, or for which they are authorized to disclose the information.

3.) Clients (providers or payers) are required to maintain reasonable and appropriate administrative, technical, and physical safeguards.

a.) The Dynamic Data Informed Consent system ensures the integrity and confidentiality of health information; and

b.) The Dynamic Data Informed Consent system protects against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information.

4.) All uses and disclosures are restricted, to the extent practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

5.) Clients (providers and payers) are required to prepare a written notice to inform patients of their information practices and of patients' rights regarding the health information.

6.) Patients are allowed to inspect and copy health information about them held by providers and payers (and by) public health authorities, and by oversight agencies in any situation in which an oversight agency has made an adverse decision about the rights, benefits, or privileges of the patient.

7.) Patients are permitted to seek correction or amendment of health information about them held by any entity obliged to permit patients to inspect health information about them.

8.) Clients (providers and payers) are required to retain a history of all disclosures of health information made for treatment, payment, research, oversight, public health, emergencies, to State data systems, for law enforcement, in judicial proceedings, and with the authorization of the patient. The record includes the date and purpose of the disclosure; the name and address to whom the disclosure was made or the location to which the disclosure was made; and where practicable, a description of the information disclosed. Patients are permitted to see this record and the disclosure history is maintained for the life of the record to which it relates.

9.) Clients (providers and payers) are permitted to disclose information pursuant to the authorization of a patient under the following conditions:

a.) The authorization is in writing, is dated, and is signed or otherwise authenticated;

b.) The authorization states an expiration date, or event, and is received by that date or event;

c.) The authorization specifies the information to be disclosed;

d.) The authorization specifies the entity or entities which are to disclose the information;

e.) The authorization specifies the person or persons or entity or entities to receive the information;

f.) The authorization states that the patient has received a statement of the intended use of the information by the recipient; and

g.) The authorization is not on the same form on which a patient consents to health care.

10.) Clients (providers and payers or other persons) who request a patient to authorize disclosure of health information are required to give the patient a copy of the authorization.

11.) A consumer is permitted to revoke an authorization to disclose information except to the extent that action has been taken in reliance on the authorization.

12.) Entities disclosing information pursuant to an authorization are required to retain a copy of the authorization, and a record of the disclosure.

13.) A person who requests a consumer to authorize disclosure of health information is required to provide a statement for retention by the patient, not on the

same form as the authorization for treatment, specifying the purposes for which the information is sought and the uses and disclosures to be made of it. The use or disclosure of the health information inconsistent with the statement is the basis for a civil action for damages.

Requirements of Data Informed Consent

To convert the principles noted above into a functional Data Informed Consent that, when combined with the stipulations of Digital Certificate issuance to client companies, creates a compliant transaction environment, requires that Data Informed Consent:

1.) Tell a consumer about their rights under the law, and the responsibilities of parties using their proprietary consumer specific data ("General Information").

2.) Inform the consumer of the manner in which their proprietary consumer specific data is used, managed and protected ("Specific Information") by the parties using their proprietary consumer specific data.

3.) Provide for interactive consumer control for disclosure authorization and the revocation thereof ("Dynamic Consent").

In other words, Data Informed Consent articulates what the Dynamic Data Informed Consent system client companies will do (under the Dynamic Data Informed Consent system watchfulness), and does what the Dynamic Data Informed Consent system's consumers authorize be done with their proprietary consumer specific data - hence a two-way interaction: the Dynamic Data Informed Consent system informs; consumers consent. It is the consent side that involves the interactive programming and the functionality of Data Informed Consent to monitor and authorize the completion of health care data transactions by third parties that involve Data Informed Consent subject proprietary consumer specific data.

Excerpting from the proposed Health and Human Services regulations, the following functional elements can be categorized as either achieving compliance through informing or achieving compliance via managing consent:

1.) Elements that proscribe a duty to inform include 1 – 5.

2.) Elements that proscribe a duty to manage consent include 8 – 13.

3.) Elements that speak to access to records include 6 – 8.

The Dynamic Data Informed Consent system intends to provide its consumer

customers with services that allow the Dynamic Data Informed Consent system to act as consumers' agent in gaining such access. The Data Informed Consent module application itself is both explanatory and interactive, taking into account the functionality dictated by the proposed regulations.

Basic Components of the Dynamic Data Informed Consent System

The components of the Dynamic Data Informed Consent system by which dynamic Data Informed Consent modulates a security structure for the transmission and exchange of personal electronic data include:

A public key infrastructure (PKI) that provides robust encryption of all data routed through the Dynamic Data Informed Consent system. Encryption modalities other than PKI may be employed to implement this function.

Digital certificates to provide ongoing authentication of approved parties, and associated constraints on use and attestations provided by the parties to whom they are issued. Other means of authentication such as passwords, biometrics and smart cards may be used to implement this function.

A data center and service center managed by a controlling entity to manage both the issuance of digital certificates to participants (client companies and consumers), and the management of Data Informed Consent.

The Data Informed Consent module and methods of management as a governor of the transaction environment. The Data Informed Consent module consists of a rules-driven (inference engine-driven) database management system (DBMS) with lookup tables corresponding with the authorizations, or revocations thereof, placed by each consumer executing Data Informed Consent.

The Data Informed Consent module itself consists of the following essential elements:

A cross-platform compatible, scalable data base management system (DBMS) such as Oracle or Sybase.

A graphic user interface to allow consumer interaction with the Dynamic Data Informed Consent system.

A forms-driven mechanism for the consumer to understand their legal rights and to modify authorizations for various consumer-specified entities to

hold, access and transact with (disclose) the consumer's proprietary consumer specific data.

A component to enable the consumer to change the level of authorization to and among authorized parties so as to enable the consumer to segmentalize (compartmentalize) proprietary consumer specific data.

Look-up tables with reference to individual consumers that list authorizations and similar tables that consist of revocations of authorizations.

A component to enable log all instances of authorized use of proprietary consumer specific data and unauthorized attempts to use proprietary consumer specific data.

Software to audit and analyze the logs that catalogue authorized and attempts at unauthorized use of proprietary consumer specific data.

Software interface with PKI or other data security platform such that consumer identifiers are accessed and checked against authorization and authorization revocation lists.

Operation of the Dynamic Data Informed Consent System

Figure 2 illustrates additional details of the Dynamic Data Informed Consent system 101 in conceptual block diagram form to illustrate the functionality of this system. The Dynamic Data Informed Consent system 101 is shown interconnected by a data communication medium 201 with a plurality of clients and consumers. In particular, a plurality of consumers can access the Dynamic Data Informed Consent system 101 via their data terminal devices 211-213 to subscribe to the services of the Dynamic Data Informed Consent system 101, establish a data informed consent for storage therein and optionally to dynamically update the data informed consent. The clients represent various users, such as Information Management System (IMS2), who store proprietary consumer specific data for the consumers, as well as clients who request access to the stored proprietary consumer specific data. In the health care example used herein, these clients can be: physicians at their data terminal devices 202; institutions, such as health care businesses, via their computer systems 280; and the like.

The Dynamic Data Informed Consent system 101 functions to regulate the

exchange of proprietary consumer specific data among the plurality of clients served by the Dynamic Data Informed Consent system 101. The Dynamic Data Informed Consent system 101, in a typical embodiment, itself comprises one or more servers 221, 222 which interface the Dynamic Data Informed Consent system 101 to the data communication medium 201. The Dynamic Data Informed Consent system 101 can be viewed as a plurality of components, which can be implemented as an integrated facility or portions thereof can be outsourced to other vendors. For example, the data storage function can optionally be implemented within Dynamic Data Informed Consent system 101 as an Information Management System (IMS1), and the Public Key Infrastructure (PKI) can optionally be implemented within Dynamic Data Informed Consent system 101. The Information Management System (IMS1) includes a data storage manager 251, administrator interface terminal 254 and its associated data storage devices 252, 253, which stores the proprietary consumer specific data. The core element of the Dynamic Data Informed Consent system 101 is the dynamic Data Informed Consent Management system (DIC Management). The Public Key Infrastructure (PKI) comprises a subscriber manager 220 and a key management element 230, shared between the Data Informed Consent Management system (DIC Management) and the Public Key Infrastructure (PKI). in addition, the Public Key Infrastructure (PKI) includes a digital certificate processing element 240.

The Data Informed Consent Management system (DIC Management) typically comprises one or more servers 221, 222 to manage interactions with the data communication medium 201. The Data Informed Consent Management system (DIC Management) includes a consumer/client subscription module comprising the RA Control Center 225, an associated administrator data terminal device 226 and data storage elements 227. Similarly, a digital certificate module, comprising the CA Control Center 223, an associated administrator data terminal device 224 and data storage elements 228, is provided. Finally, the Data Informed Consent Management system (DIC Management) includes a data informed consent module 260, comprising DIC Control Center 261, an associated administrator data terminal device 262 and data storage elements 263, 264. The operation of these elements is described below.

Dynamic Data Informed Consent Transaction

For clients and consumers to be served by the Dynamic Data Informed Consent system 101, their identity must be verified and ensured in future transactions. This is typically accomplished by use of the well known paradigm of Digital Certificates. When a consumer or client wishes to avail themselves of the services of the Dynamic Data Informed Consent system 101, they establish a communication connection via data communication medium 201 to the Dynamic Data Informed Consent system 101 and interconnect with servers 221, 222. The Dynamic Data Informed Consent system 101 then executes a script via RA Control Center 225 and certificate processing system 240, to identify the consumer/client and record their identity and set of permissions in the registration database stored in memory 227. The Dynamic Data Informed Consent system 101 in well known fashion issues a Digital Certificate via certificate processing system 240, which Digital Certificate is transmitted via servers 221, 222 and data communication medium 201 to the customer/client to thereby authorize future access to the Dynamic Data Informed Consent system 101.

When Digital Certificates are issued by the Dynamic Data Informed Consent system 101 to clients (Transacting Party A and Transacting Party B, both members of the class of clients shown in Figure 1), these parties can access the Dynamic Data Informed Consent system 101 to assure compliance with a consumer's dynamic data informed consent when accessing consumers' proprietary consumer specific data. The consumers are also provided with Digital Certificates, which they use to access the Dynamic Data Informed Consent system 101 to create the Data Informed Consent for the consumer's personal data. Thus, the consumer, via data communication medium 201, accesses the Dynamic Data Informed Consent system 101 and, in particular, the Data Informed Consent module 260 to create a Data Informed Consent file for the consumer's proprietary consumer specific data which is stored in informed consent database memory 263. This data informed consent data created by the consumer is the basis of empowering the clients to access, exchange and process the consumers' proprietary consumer specific data. It is apparent that the consumer can create the data informed consent data via the submission of a paper form, which is then input into the Dynamic Data Informed Consent system 101 by clerical staff. In either case, the data informed consent stored in Dynamic Data Informed Consent system 101 is the basis for the transactions described herein.

To follow the flow of a typical transaction involving personalized health data, consider the following example, which is illustrated in flow diagram form in Figures 3 and 4. In a typical transaction, a Transacting Party A, such as a physician at data terminal device 202, wishes to send consumer-specific data stored in Information Management System IMS2 to Transacting Party B, such as the health care business served by computer system 280. Prior to this transaction, at step 301A, Transaction Party A receives a Digital Certificate issued by the Dynamic Data Informed Consent system 101 and at step 301B Transaction Party B receives a Digital Certificate issued by the Dynamic Data Informed Consent system 101 to thereby authorize their access to the proprietary consumer specific data managed by Dynamic Data Informed Consent system 101. At step 302, Transaction Party A (the sender, often a provider) batches a plurality of customer billings for transmission to Transaction Party B (the recipient, often a payer), with attachments comprising proprietary consumer specific data stored in Information Management System IMS2, and/or requiring the Transaction Party B to access consumer medical history data stored in Information Management System IMS2. The data, regardless of application, is encrypted at step 303 under the PKI, by the Transaction Party A with digital signature attached. The data is packaged (encrypted, digital signature attached, along with statement of purpose and description of data type) by the sender Transaction Party A at step 304. Under PKI security, the data package is routed at step 305 via data communication medium 201 or other suitable medium to the Dynamic Data Informed Consent system 101.

The Dynamic Data Informed Consent system 101 Certificate Processing module 240 verifies the authorization of Transaction Party A at step 306, and the validity of Transaction Party B as a client of the Dynamic Data Informed Consent system 101. The verified request is then reviewed at step 307 to ensure that the digital signature appended to the data is correct. The data package is then routed at step 308 through the Data Informed Consent module 260 to be processed. The received request is reviewed at step 309 as to content and use requested and compared to the permissions provided by the consumer's dynamic data informed consent stored in informed consent database 263. Should a transaction party be on the Certificate Revocation List (CRL), the transaction is refused by the Dynamic Data

Informed Consent system 101 at step 310 and a record kept of the attempt to access proprietary consumer specific data, and refusal to confirm/allow in transaction audit log 264. All transactions, once cleared through the Certificate/signature validation step 309, are routed through the Data Informed Consent module 260 which at step 311 looks up the authorization status for each subject of the transaction data package. If each consumer has authorized each transaction party to receive or hold the consumer's proprietary consumer specific data, the transaction is fully cleared at step 312 and the appropriate audit log entries are recorded at step 313 in transaction audit log 264. If one or more consumers has refused (revoked) disclosure authorization to either transacting party, or if one or more consumers have not specifically authorized either transacting party, proprietary consumer specific data for those consumers is made unreadable to the recipient at step 314, and the transaction only partially cleared at step 315. An audit log is kept of each transaction for each consumer. The cleared transaction is sent on to recipient, Transaction Party B, over the data communication medium 201 at step 316. The recipient uses its private key to "unlock" the cleared transaction data package at step 317 and subject the proprietary consumer specific data to further processing. Each consumer for whom the controlling entity holds Data Informed Consent proxy also receives a Digital Certificate for authentication for entry into the consumer's own Data Informed Consent file for changes, to see transaction audit trails, etc at step 318.

In this example, there can optionally be a need to access proprietary consumer specific data which is stored in an Information Management System IMS2, which can be located external to the Dynamic Data Informed Consent system 101. In this case, the Dynamic Data Informed Consent system 101 must issue a Digital Certificate to the Information Management System IMS2 to enable the Transaction Party A and/or B to retrieve the consumers' proprietary consumer specific data and provide same to the Transaction Party B.

If Transaction Party B had requested the proprietary consumer specific data from Transacting Party A (as opposed to Transaction Party A sending the data to Transaction Party B, such as in the present example whereby Party A, a provider, might be billing Party B, a payer, for services rendered to consumers), the Dynamic Data Informed Consent system 101 could easily be used to validate the request for

appropriate authorizations, though the transaction including "wrapped" data would also need to go through the Dynamic Data Informed Consent system 101 for final validation and audit trail construction.

Information Management System Data Access Example

There are numerous clients that can access the information management system IMS2. The block diagram of Figure 6 illustrates an access of Information Management System 2, absent the interposed function the Dynamic Data Informed Consent system 101 described above to regulate access to the proprietary consumer specific data. This description is intended to illustrate a typical implementation of an Information Management System IMS2 which can be cooperatively operative with the Dynamic Data Informed Consent system 101 as described above.

The data accessing clients include health care providers at their terminal equipment or servers S1-Sm, institutions via their terminal equipment and servers I1-Ij, and the like. The various users each can use the communication network PTSN to access the information management system IMS and its analysis function based upon the predefined class of "users" which classes can include consumers, medical practitioners, health care providers, institutions, and the like. The database 400 is architected in a hierarchical manner to enable the users to access only the relevant, prepartitioned segment of the collected proprietary consumer specific data that the particular class of user is authorized to receive. Thus, the privacy of the proprietary consumer specific data is maintained by prohibiting access to this individual's proprietary consumer specific data except to users who are specifically authorized by the consumer. In addition, the granularity of the proprietary consumer specific data made available to the various classes of users is selected to prevent the users from deriving information about the consumer population that they are not entitled to receive. This access control is enforced by the use of a plurality of filters 403-406, each of which is architected to provide customized access to a selected one of the classes of users that can access the information management system IMS, as described below.

Information Management System Architecture

The information management system IMS comprises a database 400 that stores and manages the proprietary consumer specific data collected from the

consumers. The proprietary consumer specific data is typically stored in database 400 on a mass storage system to enable the associated database processors to have efficient shared access to this data. The database processors include data processing algorithms 408 that operate on the proprietary consumer specific data that is collected from the individual consumers to produce additional data that is indicative of consumer specific or user specific statistics.

Once acquired, the proprietary consumer specific data may serve a multitude of inquisitors. Assigning a user-access code to each class of inquisitor easily controls level of access and interpretation. The interpretation filters 404-406 are specific to each class of user-access code. The users who are entitled to access to the system are:

Consumers who have registered

Physician care-providers who are registered as subscribers

Institutions who are registered as subscribers

Each user is assigned an access code. The system database includes various data segments including, but not limited to:

Raw data

Demographic, user-specific data

User access codes

Database Management System

The database management system that is operational on the database 400 comprises analytical software that includes both the commercially available database software and custom software for the specific data analysis task. The software routines include but are not limited to:

Access Code Recognition Software 401 - verifies that the inquiring user has an operative access code, confirms the code classification and routes the user's request to an Initial Output Filter

Download Acceptance Software 402 - accepts data for storage in the database, places the received data in a buffer file until the received data can be screened and processed for inclusion in the database

Initial Output Filter 403 - segregates the possible array of outputs as a function of access code and query.

Pattern Recognition Software 407 - an artificial intelligence routine that takes the elements of a pattern and compares the pattern against known patterns to produce an analysis result within certain confidence limits.

Consumer Query Output Filter 404 - this routine delimits the nature of the output report to the consumer.

Provider Query Output Filter 405 - this routine delimits the nature of the output report to the provider.

Institution Query Output Filter 406 - this routine delimits the nature of the output report to the institution.

Institution Query

An example of the use of the information management system IMS is where an institution, such as a managed care company, seeks information regarding fertility status among a population of reproductive age women in the New York state area, where the company is considering offering coverage for infertility care. In order to assess the economics of such coverage, the institution needs accurate actuarial data on the type of fertility problems exist and the frequency of such problems. Figure 6 illustrates the communication pathways that are used in the processing of an institution query to the information management system IMS, while Figure 7 illustrates in flow diagram form the operation of this information management system IMS.

At step 701 the institution activates the telecommunications software resident in the institution's personal computer 500 to establish a communication connection to the Web Site Router 200 over a standard communication connection via path (a). Once so connected, the personal computer 500 identifies itself by transmitting the institution's Institution Access Code and a request for information to the information management system IMS. At step 702, the Web Site Router 200 receives the request and forwards the received query over path (b) to the database 400. At step 703, the database system 400 activates the access code recognition process 401 which compares the received institution access code data with institution data stored in the database 400 to verify the both the nature of the requesting party (institution) and the authorization of this institution to access the services and data provided by the database 400. Once the institution is validated, the access code recognition process 401 forwards the received request over path (c) to the initial output filter 403. The

initial output filter 403 at step 704 determines the nature of the query, which can be a query that was selected from a set of standard queries or one constrained to a predefined format to ensure privacy of the consumer-specific data, and approves the generation of a demographic report to the institution. The is accomplished at step 705 by transmitting the query that is received from the institution in the proper format to the AI Pattern Recognition Subroutines 407 via path (d). At step 706, the AI Pattern Recognition Subroutines 407 process the data resident in the Data Tables, Files and Records portion 408 of the database 400, which data is accessed via path (e). The data processing retrieves the demographic data and processes the raw data that is stored in the database 400 and the AI Pattern Recognition Subroutines 407 produces a result that typically comprises a set of composite statistics. At step 707, the AI Pattern Recognition Subroutines 407 transmits this information via path (f) to the Institution Query Output Filter 406 which at step 708 determines the proper formatting and additional data that is needed to produce a report for the institution. As part of this process, the Institution Query Output Filter 406 verifies that the data retrieved is not consumer-specific or of such limited scope as to compromise the privacy of the consumer-specific data. This process includes a determination of the size of the sample cohort, its respective size with respect to the overall target population, the topic areas that this institution is authorized to access, the specifics of the query, and the like. At step 709, the Institution Query Output Filter 406 transmits this final report via path (g) to the Web Site Router 200 which forwards the report at step 710 to the institution's personal computer 500 via path (h) for viewing.

Data Download Validation

In order to ensure the integrity of the data that is stored in the database 400, the information management system IMS includes a download acceptance process 402 that receives data that is transmitted to the information management system IMS and stores the data via path (x) in a temporary file termed "data on hold 409" until the data can be validated. The validation process comprises a review of the format and content of the data to prevent bogus data from corrupting the integrity of the database 400. In particular, the user identification information as well as the associated data is screened for data usability and associated demographic information. The proper formatting of the data is verified and then the received data is stored in the data on

hold file 409. Once the data stored in this file is reviewed by either information management system IMS personnel and/or further validation software, it is downloaded via path (y) to the permanent data repository of data tables, files and records 408 where it is incorporated into the existing population of data.

Domain Definition for the Dynamic Data Informed Consent System

Figure 5 illustrates in block diagram form the structure of the Dynamic Data Informed Consent Domain. In particular, the correspondence among the various data elements in the Dynamic Data Informed Consent system is illustrated. Thus, the consumer has a one to one mapping to a Data Informed Consent, since the Dynamic Data Informed Consent system maintains a single Data Informed Consent for each consumer. The Data Informed Consent is mapped to up to n clients, although at any time there may be no clients authorized under the consumer's Data Informed Consent. Similarly, the consumer has a one to one correspondence to an audit trail file maintained by the Dynamic Data Informed Consent system. The audit trail file is mapped to up to n Data Informed Consent Updates, although at any time there may be no Data Informed Consent Updates authorized under the consumer's Data Informed Consent. The Data Informed Consent Updates are mapped to up to n clients, although at any time there may be no clients authorized under the consumer's Data Informed Consent Updates. The consumer's audit trail file is mapped to up to n Health Information Transactions, although at any time there may be no Health Information Transactions authorized under the consumer's Data Informed Consent. Similarly, each Health Information Transaction is mapped to up to n transmitting and n receiving clients, although at any time there may be no clients authorized under the consumer's Data Informed Consent.

Client Use Cases

Client use cases are uses that may require internal dynamic Data Informed Consent controls. In these instances, each consumer, via the Dynamic Data Informed Consent system's Data Informed Consent mechanism, has authorized a health care company (e.g., a hospital) to use their proprietary consumer specific data internally. In a hospital setting, uses may include sending clinical laboratory or X-ray data to the patient's record, compilation of admission, discharge and transfer (ADT) data for billing purposes (ICD-9 and CPT codes), sending clinical data for in-house pharmacy

use, providing clinical data to and for exchange among treating physicians under hospital contract, etc. Other examples in which internal data exchange might be covered with transaction-by-transaction Data Informed Consent management include those entities that provide partially or fully integrated health care delivery (e.g., when a physician group owns a hospital and associated laboratory, surgical center, clinic, etc., under the umbrella of a single business entity; or a fully integrated [payer + provider] entity).

In all circumstances, Data Informed Consent is a given, though internal granularity of authorized data movement may be governed under a broader Data Informed Consent, together with a PKI/Digital Certificate set of controls and with appropriate security/privacy policy and procedures. Also, any proprietary consumer specific data transferred out of the entity to any other party would automatically default to full PKI/Data Informed Consent compliance monitoring by the Dynamic Data Informed Consent system's external, Web-based system.

Different levels of authorization are likely to be operative in the integrated delivery environment. For example, separate Digital Certificate and Data Informed Consent constraints might be applied to: Provider to provider exchange of clinical data; Other client company personnel processing of personalized health care data; New uses of data such as outcome research or pharmacy benefits analysis.

Uses That Involve Dynamic Data Informed Consent Controls

When personalized health care data is exchanged between independent business entities (e.g., a hospital sending patient billing to a payer or fiscal intermediary), both businesses are required to be in compliance with the privacy/security law. The Dynamic Data Informed Consent system's Data Informed Consent manages the traffic on the PKI by checking data for Data Informed Consent compliance as it is routed through the Dynamic Data Informed Consent system Data Center. The actual processing performed by the Data Informed Consent module is transparent to the transacting parties (provider and payer). Each of them uses the Dynamic Data Informed Consent system PKI and their respective Digital Certificate's to package, encrypt and then unlock the data. Data Informed Consent management takes place en route.

Other Uses of Dynamic Data Informed Consent Controls by Clients

Personalized health care data may legitimately be used outside the scope of health care operations for research, for market assessment, for direct marketing, for public health reporting, for law enforcement purposes, for quality assessment of care delivery, etc. Aside from public health reporting and law enforcement where separate disclosure is mandated by law, every use of personalized health data beyond the context of healthcare operations must be sanctioned (authorized) by those to whom the data pertains. The Dynamic Data Informed Consent system accommodates these special use cases via its dynamic Data Informed Consent offering.

The Dynamic Data Informed Consent System Administrative Use Cases

Typical examples of the use of the Dynamic Data Informed Consent system include, but are not limited to the functions listed herein:

Enroll and authenticate consumer

Verify Data Informed Consent status

Issue Digital Certificate to consumer (in conjunction with Data Informed Consent)

Assist consumer with Data Informed Consent changes

Periodically verify consumer information

Renew consumer Data Informed Consent

Service data access and audit trail requests by consumer

Obtain, on customer's behalf, customer's data held by others

Service audit log access requests by client companies

Authenticate client companies

Issue Digital Certificates (and sub-certificates) to clients and their employees

Verify client companies' authorized access to consumer information

Consumers' Component

The consumer's component of the Data Informed Consent application is installed in a manner similar to common consumer applications for personal computers. Default values for all installation parameters are provided to effect a correct installation on a personal computer with sufficient disk space, an Internet connection, and no other application programs running on the computer at the time of installation.

A program for uninstalling the Data Informed Consent application is also

installed on the personal computer during the Data Informed Consent application's installation. The consumer is able to remove the Data Informed Consent application from the computer using this program.

If, for some reason, the installation of the Data Informed Consent application is unsuccessful (if, for example, there is insufficient disk space), the installation program removes all installed and partially installed components of the Data Informed Consent application from the computer.

Client Workers' Component

The client workers' component of the PKI/Data Informed Consent application is installed in a manner similar to common business-office software. It is possible for system administrators to install the application on workers' computers from a central server, or on the target computer directly. Installation and uninstallation may require administrative privileges.

Summary

The Dynamic Data Informed Consent system enables consumers to govern the flow of their personal data regardless of the nature of the information. The consumer can define a set of data access rules which designate the client companies who have access to the consumer's personal data and the particular segments of that personal data to which each client company is entitled. The Data Informed Consent is dynamic in that the consumer can use their Digital Certificate at any time to access and modify their Data Informed Consent provided to the Dynamic Data Informed Consent system.

What is Claimed:

1. An interactive information management system for regulating users' access to proprietary consumer specific data, comprising data that relates to each of a plurality of consumers, where said proprietary consumer specific data is stored in a data storage system, comprising:

means for storing dynamic data informed consent data, comprising a set of rules which govern a transaction environment for the exchange of proprietary consumer specific data by and among users; and

means for authorizing an accessing user to receive dynamic data informed consent access to said proprietary consumer specific data.

2. The interactive information management system of claim 1 further comprising:

means, responsive to a consumer accessing said interactive information management system, for generating for said consumer dynamic data informed consent data comprising a set of rules which govern a transaction environment for the exchange of proprietary consumer specific data by and among users.

3. The interactive information management system of claim 2 wherein said means for generating comprises:

means for informing said consumer that there is the possibility of collection of proprietary consumer specific data relating to said consumer.

4. The interactive information management system of claim 2 wherein said means for generating comprises:

means for enabling said consumer to prevent collection, disclosure or exchange of said proprietary consumer specific data relating to said consumer.

5. The interactive information management system of claim 2 wherein said means for generating comprises:

means for informing said consumer how said proprietary consumer specific

data, relating to said consumer and stored in said data storage system is expected to be used; and

means for instructing said consumer how to restrict use of said proprietary consumer specific data, relating to said consumer and stored in said data storage system.

6. The interactive information management system of claim 2 wherein said means for generating comprises:

security means for informing said consumer of the extent to which said proprietary consumer specific data, relating to said consumer and stored in said data storage system is protected.

7. The interactive information management system of claim 2 wherein said means for generating comprises:

consumer correction means for enabling a consumer to correct inaccuracies in said proprietary consumer specific data, relating to said consumer and stored in said data storage system.

8. The interactive information management system of claim 2 wherein said means for generating comprises:

means for generating a digital certificate to enable said consumer future access to said interactive information management system.

9. The interactive information management system of claim 1 wherein said means for providing dynamic data informed consent access comprises:

means for enabling a consumer to authorize at least one user to access proprietary consumer specific data, relating to said consumer and stored in said data storage system.

10. The interactive information management system of claim 1 wherein said means for providing dynamic data informed consent access comprises:

means, responsive to a user requesting access to proprietary consumer specific data, relating to an identified consumer and stored in said data storage

system, for determining an identity of said user;

means for comparing said identity with said dynamic data informed consent data to verify said user's authority to access said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system; and

means for generating a digital certificate which identifies said user and defines limits of said user's authority to access and use said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system.

11. The interactive information management system of claim 1 further comprising:

means for tracking user access to and exchange of said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system.

12. The interactive information management system of claim 1 wherein said means for providing dynamic data informed consent access comprises:

means for enabling a user to input a query relating to proprietary consumer specific data, relating to said consumer and stored in said data storage system; and

means, responsive to said input query, for blocking intrusive access to said proprietary consumer specific data, relating to said consumer and stored in said data storage system, by said user inputting said query.

13. The interactive information management system of claim 12 wherein said means for blocking intrusive access comprises:

a plurality of input filters, each of which functions to provide limits to a quantity and content of proprietary consumer specific data, relating to said consumer and stored in said data storage system.

14. The interactive information management system of claim 1 wherein said data storage system is located external to said interactive information management system and accessible via electronic communication means.

15. The interactive information management system of claim 1 wherein said data storage system is a part of said interactive information management system.

16. The interactive information management system of claim 15 wherein said data storage system comprises:

electronic database means for storing said proprietary consumer specific data.

17. The interactive information management system of claim 15 wherein said data storage system includes a set of paper records.

18. A method of operating an interactive information management system for regulating users' access to proprietary consumer specific data, comprising data that relates to each of a plurality of consumers, where said proprietary consumer specific data is stored in a data storage system, comprising:

means for storing dynamic data informed consent data, comprising a set of rules which govern a transaction environment for the exchange of proprietary consumer specific data by and among users; and

means for authorizing an accessing user to receive dynamic data informed consent access to said proprietary consumer specific data.

19. The method of operating an interactive information management system of claim 18 further comprising:

means, responsive to a consumer accessing said interactive information management system, for generating for said consumer dynamic data informed consent data comprising a set of rules which govern a transaction environment for the exchange of proprietary consumer specific data by and among users.

20. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

means for informing said consumer that there is the possibility of collection of proprietary consumer specific data relating to said consumer.

21. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

means for enabling said consumer to prevent collection, disclosure or exchange of said proprietary consumer specific data relating to said consumer.

22. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

means for informing said consumer how said proprietary consumer specific data, relating to said consumer and stored in said data storage system is expected to be used; and

means for instructing said consumer how to restrict use of said proprietary consumer specific data, relating to said consumer and stored in said data storage system.

23. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

security means for informing said consumer of the extent to which said proprietary consumer specific data, relating to said consumer and stored in said data storage system is protected.

24. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

consumer correction means for enabling a consumer to correct inaccuracies in said proprietary consumer specific data, relating to said consumer and stored in said data storage system.

25. The method of operating an interactive information management system of claim 19 wherein said means for generating comprises:

means for generating a digital certificate to enable said consumer future access to said interactive information management system.

26. The method of operating an interactive information management system

of claim 18 wherein said means for providing dynamic data informed consent access comprises:

means for enabling a consumer to authorize at least one user to access proprietary consumer specific data, relating to said consumer and stored in said data storage system.

27. The method of operating an interactive information management system of claim 18 wherein said means for providing dynamic data informed consent access comprises:

means, responsive to a user requesting access to proprietary consumer specific data, relating to an identified consumer and stored in said data storage system, for determining an identity of said user;

means for comparing said identity with said dynamic data informed consent data to verify said user's authority to access said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system; and

means for generating a digital certificate which identifies said user and defines limits of said user's authority to access and use said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system.

28. The interactive information management system of claim 18 further comprising:

means for tracking user access to and exchange of said proprietary consumer specific data, relating to an identified consumer and stored in said data storage system.

29. The interactive information management system of claim 18 wherein said means for providing dynamic data informed consent access comprises:

means for enabling a user to input a query relating to proprietary consumer specific data, relating to said consumer and stored in said data storage system; and

means, responsive to said input query, for blocking intrusive access to said proprietary consumer specific data, relating to said consumer and stored in said data storage system, by said user inputting said query.

30. The method of operating an interactive information management system of claim 28 wherein said means for blocking intrusive access comprises:

a plurality of input filters, each of which functions to provide limits to a quantity and content of proprietary consumer specific data, relating to said consumer and stored in said data storage system.

31. The method of operating an interactive information management system of claim 18 wherein said data storage system is located external to said interactive information management system and accessible via electronic communication means.

32. The method of operating an interactive information management system of claim 18 wherein said data storage system is a part of said interactive information management system.

33. The method of operating an interactive information management system of claim 31 wherein said data storage system comprises:

electronic database means for storing said proprietary consumer specific data.

34. The method of operating an interactive information management system of claim 31 wherein said data storage system includes a set of paper records.

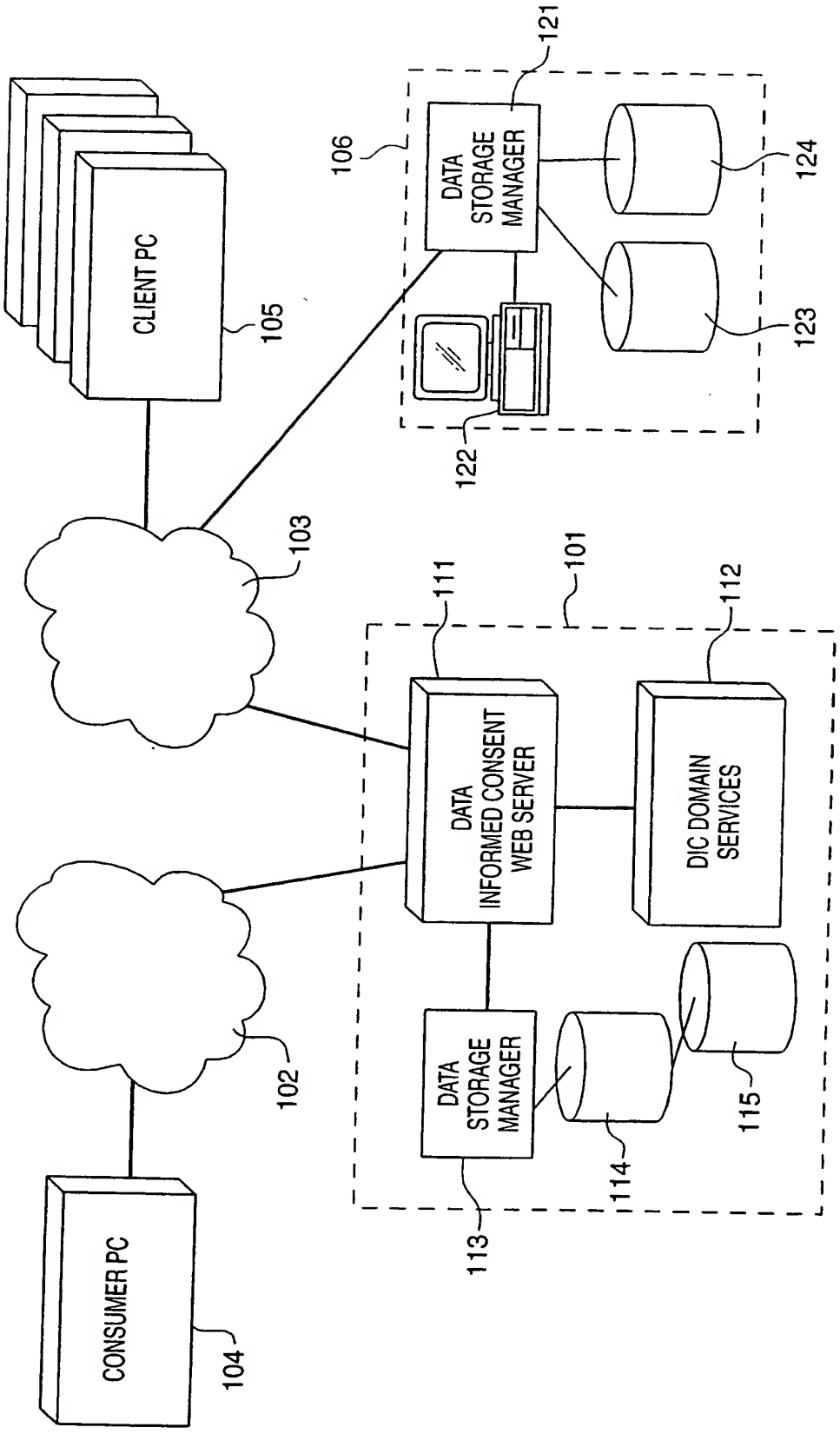

CLIENT PC
105
106
DATA STORAGE MANAGER
121
124
123
122
103
101
111
112
DATA INFORMED CONSENT WEB SERVER
DIC DOMAIN SERVICES
102
DATA STORAGE MANAGER
114
115
113
CONSUMER PC
104

FIG. 1

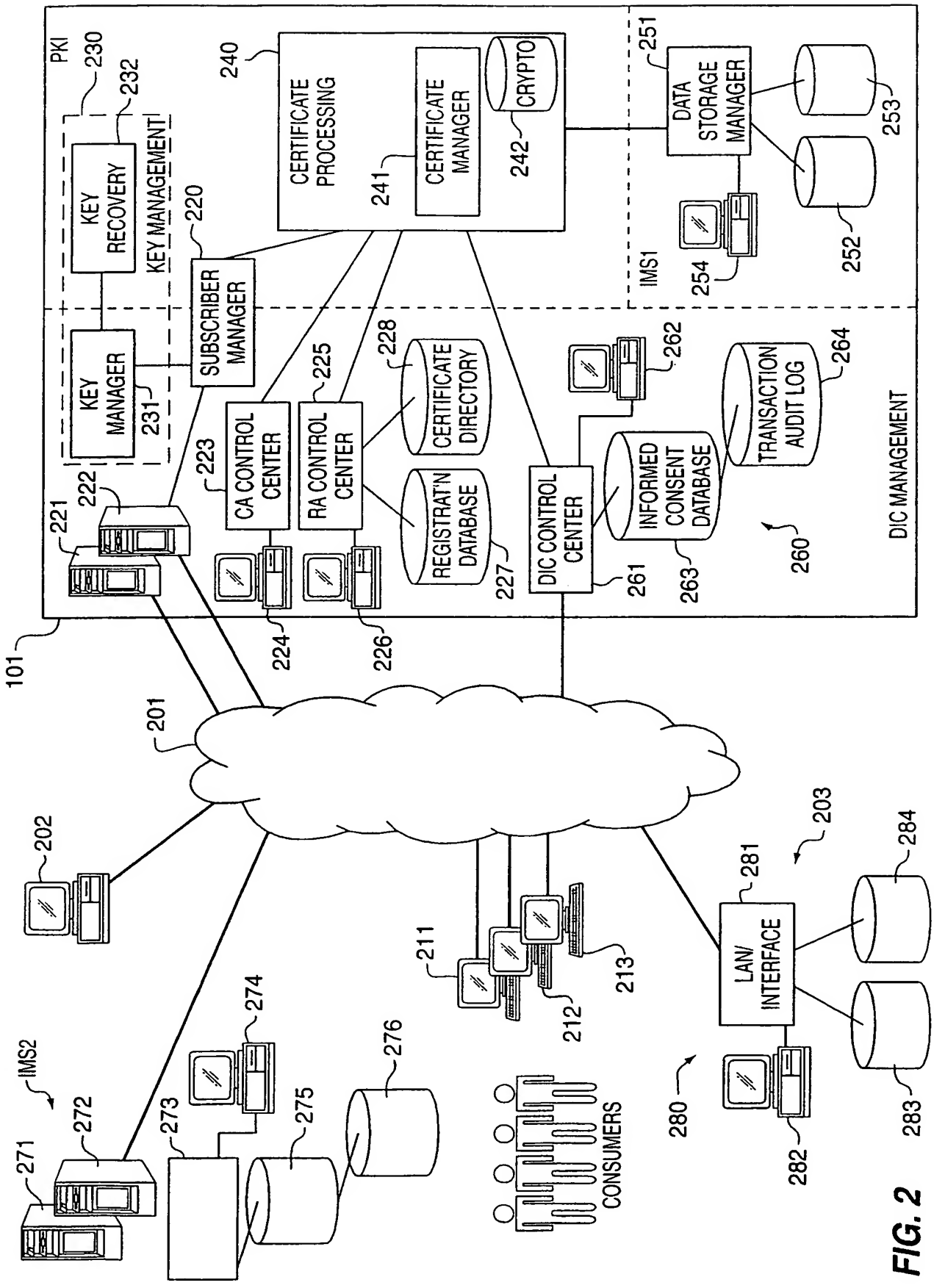

PKI
230
232
KEY RECOVERY
KEY MANAGEMENT
220
KEY MANAGER
231
SUBSCRIBER MANAGER
240
CERTIFICATE PROCESSING
241
CERTIFICATE MANAGER
242
CRYPTO
251
DATA STORAGE MANAGER
253
252
254
IMS1
221
222
223
CA CONTROL CENTER
225
RA CONTROL CENTER
228
CERTIFICATE DIRECTORY
REGISTRAT'N DATABASE
227
224
226
101
DIC CONTROL CENTER
261
262
INFORMED CONSENT DATABASE
263
TRANSACTION AUDIT LOG
264
260
DIC MANAGEMENT
201
202
203
281
LAN/ INTERFACE
284
283
282
280
211
212
213
CONSUMERS
IMS2
271
272
273
274
275
276

FIG. 2

FIG. 3

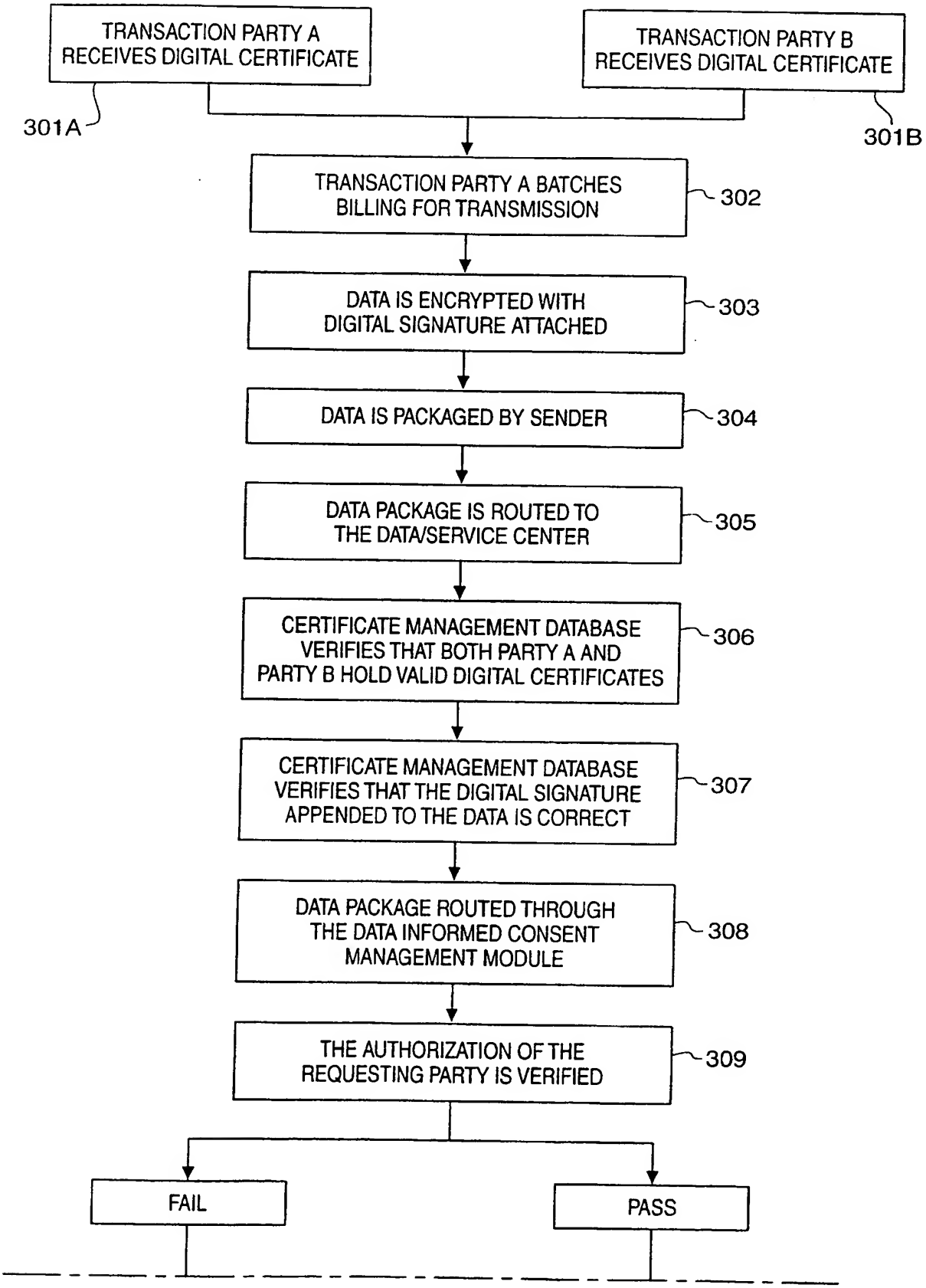
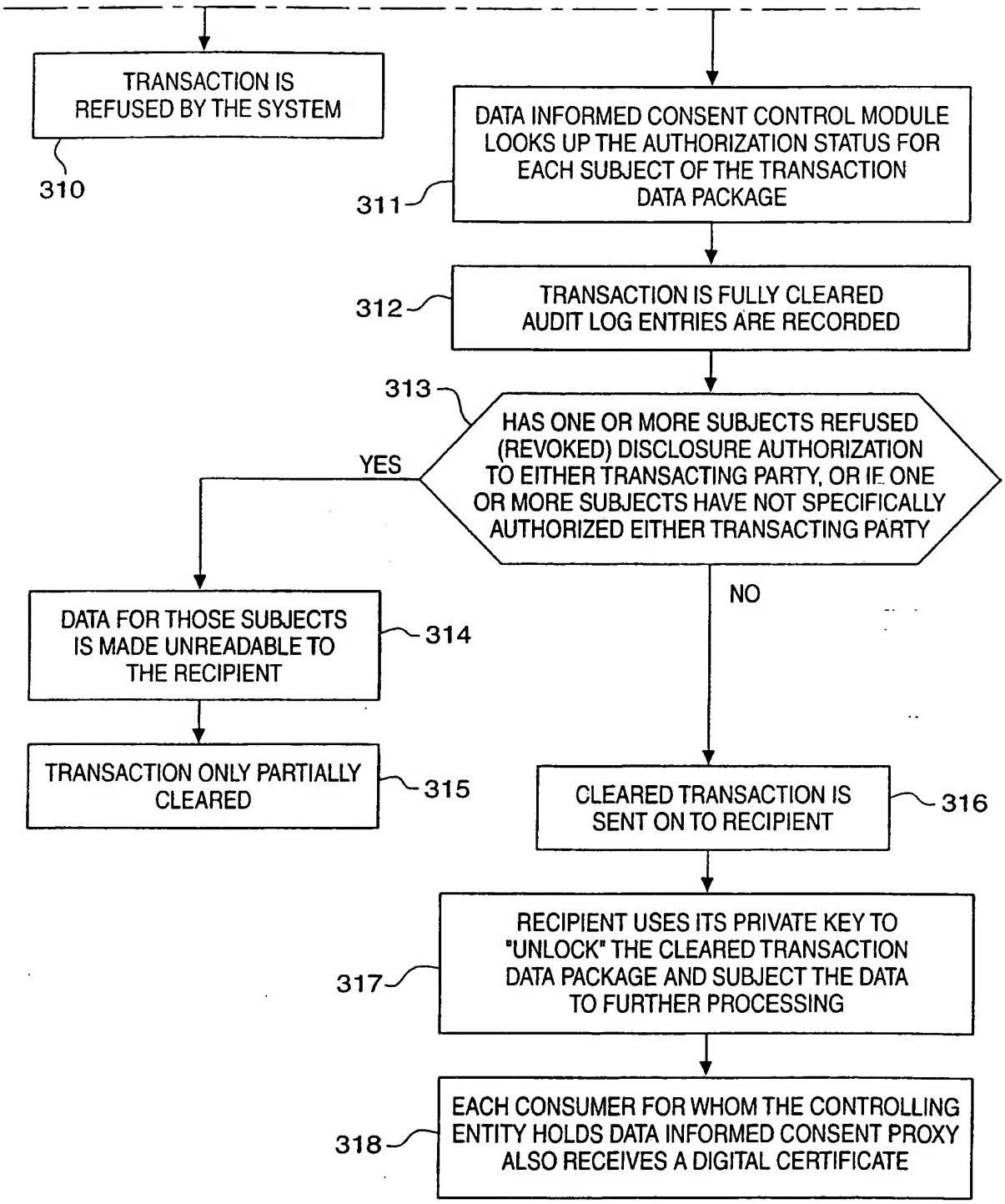

TRANSACTION PARTY A RECEIVES DIGITAL CERTIFICATE
301A
TRANSACTION PARTY B RECEIVES DIGITAL CERTIFICATE
301B
TRANSACTION PARTY A BATCHES BILLING FOR TRANSMISSION
302
DATA IS ENCRYPTED WITH DIGITAL SIGNATURE ATTACHED
303
DATA IS PACKAGED BY SENDER
304
DATA PACKAGE IS ROUTED TO THE DATA/SERVICE CENTER
305
CERTIFICATE MANAGEMENT DATABASE VERIFIES THAT BOTH PARTY A AND PARTY B HOLD VALID DIGITAL CERTIFICATES
306
CERTIFICATE MANAGEMENT DATABASE VERIFIES THAT THE DIGITAL SIGNATURE APPENDED TO THE DATA IS CORRECT
307
DATA PACKAGE ROUTED THROUGH THE DATA INFORMED CONSENT MANAGEMENT MODULE
308
THE AUTHORIZATION OF THE REQUESTING PARTY IS VERIFIED
309
FAIL
PASS

FIG. 4


TRANSACTION IS REFUSED BY THE SYSTEM
310
DATA INFORMED CONSENT CONTROL MODULE LOOKS UP THE AUTHORIZATION STATUS FOR EACH SUBJECT OF THE TRANSACTION DATA PACKAGE
311
TRANSACTION IS FULLY CLEARED AUDIT LOG ENTRIES ARE RECORDED
312
313
HAS ONE OR MORE SUBJECTS REFUSED (REVOKED) DISCLOSURE AUTHORIZATION TO EITHER TRANSACTING PARTY, OR IF ONE OR MORE SUBJECTS HAVE NOT SPECIFICALLY AUTHORIZED EITHER TRANSACTING PARTY
YES
NO
DATA FOR THOSE SUBJECTS IS MADE UNREADABLE TO THE RECIPIENT
314
TRANSACTION ONLY PARTIALLY CLEARED
315
CLEARED TRANSACTION IS SENT ON TO RECIPIENT
316
RECIPIENT USES ITS PRIVATE KEY TO "UNLOCK" THE CLEARED TRANSACTION DATA PACKAGE AND SUBJECT THE DATA TO FURTHER PROCESSING
317
EACH CONSUMER FOR WHOM THE CONTROLLING ENTITY HOLDS DATA INFORMED CONSENT PROXY ALSO RECEIVES A DIGITAL CERTIFICATE
318

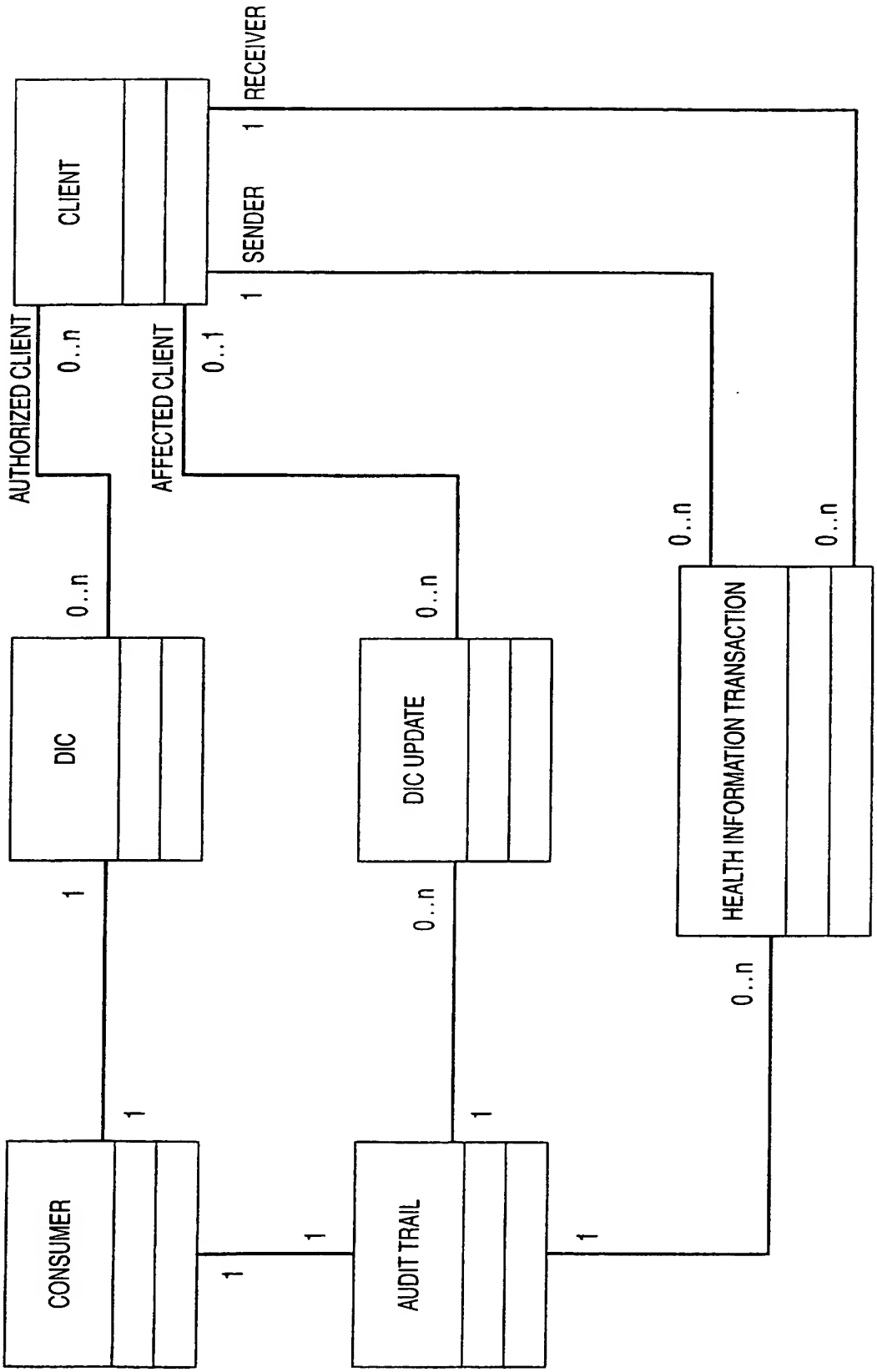

CLIENT
RECEIVER
SENDER
1
1
AUTHORIZED CLIENT
0..n
AFFECTED CLIENT
0..1
DIC
DIC UPDATE
HEALTH INFORMATION TRANSACTION
0..n
0..n
0..n
0..n
0..n
1
1
1
1
CONSUMER
AUDIT TRAIL
1
1
1

FIG. 5

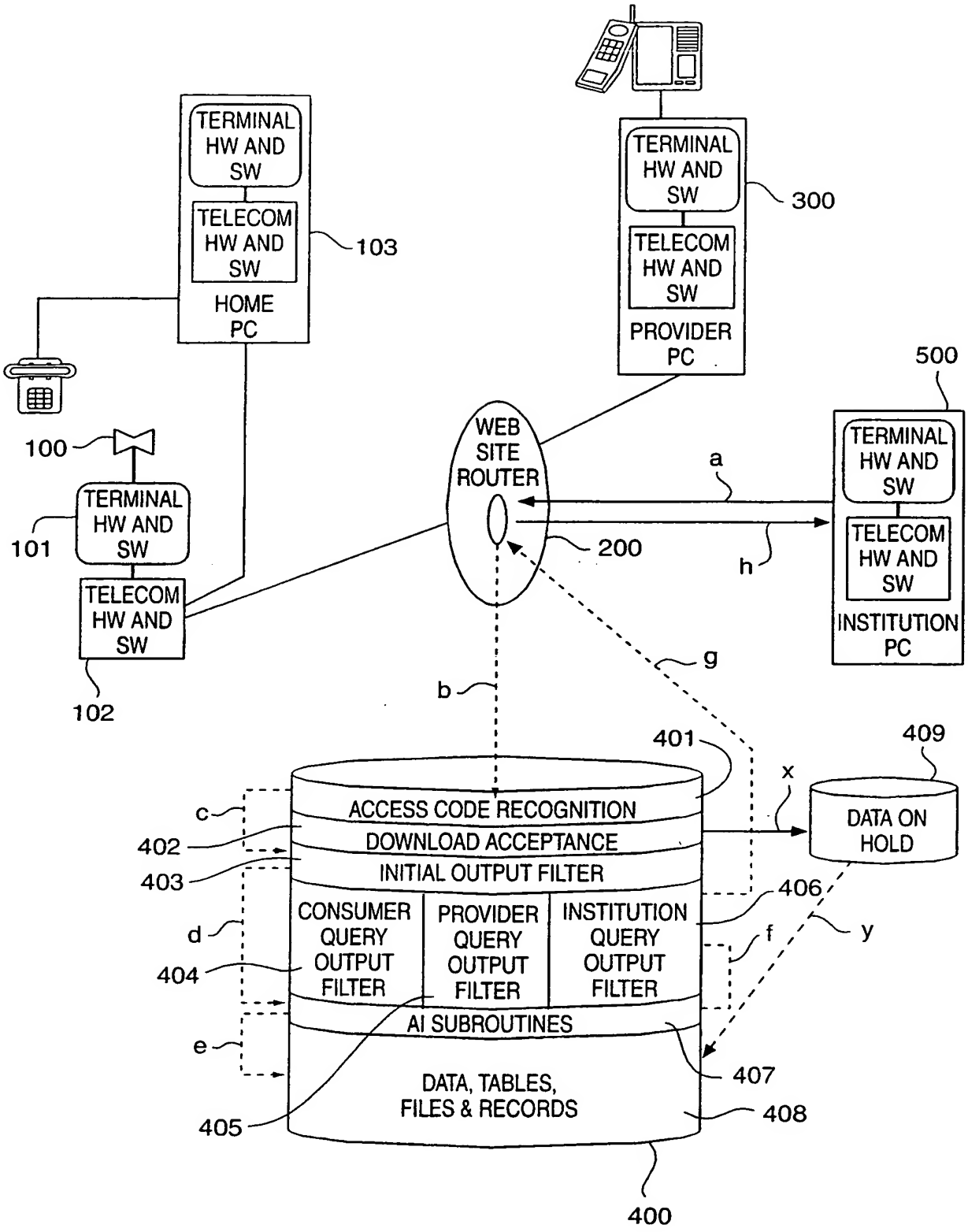
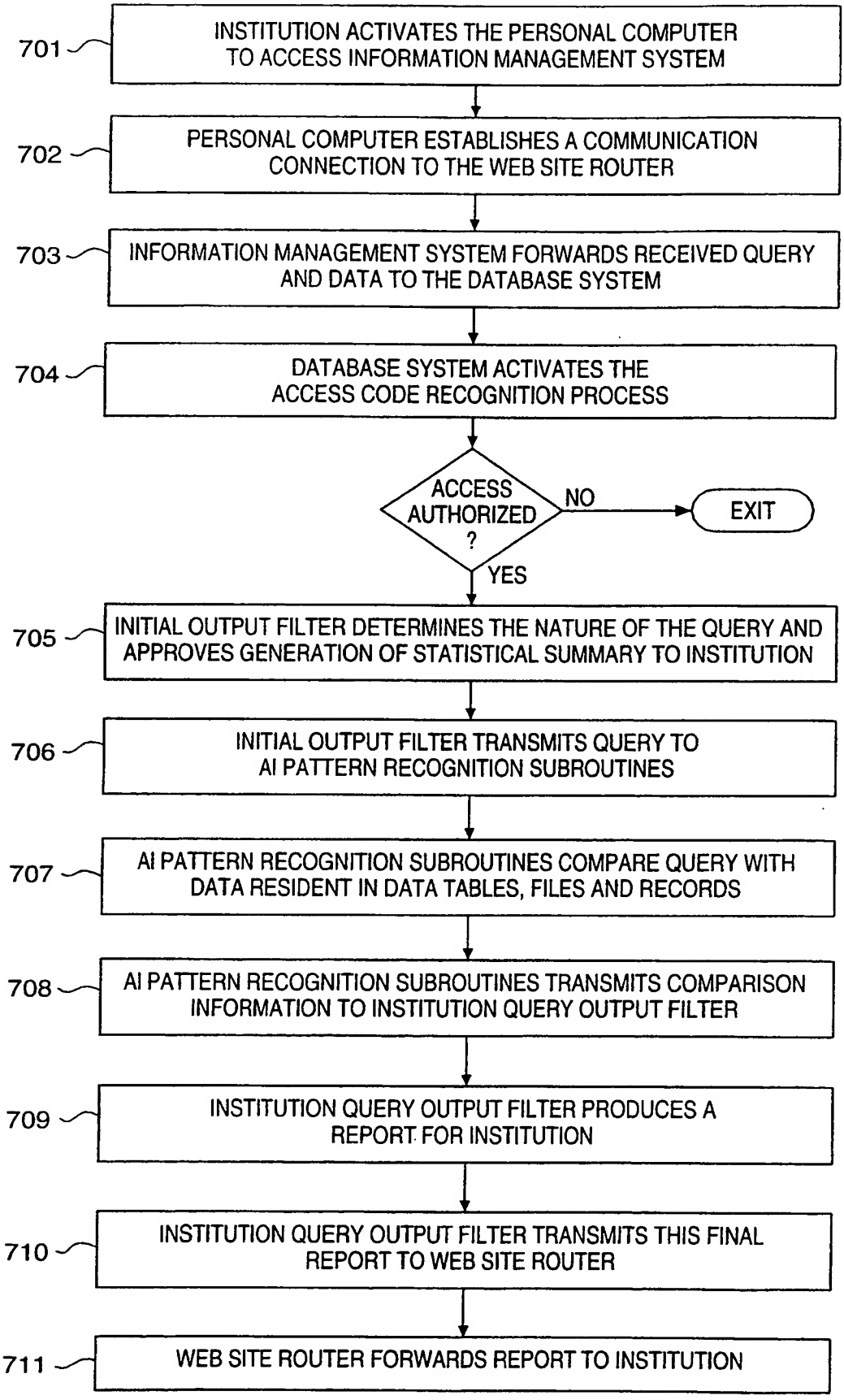

TERMINAL HW AND SW
TELECOM HW AND SW
HOME PC
103
TERMINAL HW AND SW
TELECOM HW AND SW
PROVIDER PC
300
500
100
101
TERMINAL HW AND SW
TELECOM HW AND SW
102
WEB SITE ROUTER
200
a
h
TERMINAL HW AND SW
TELECOM HW AND SW
INSTITUTION PC
b
g
401
409
x
c
ACCESS CODE RECOGNITION
DATA ON HOLD
402
DOWNLOAD ACCEPTANCE
403
INITIAL OUTPUT FILTER
406
d
CONSUMER QUERY OUTPUT FILTER
PROVIDER QUERY OUTPUT FILTER
INSTITUTION QUERY OUTPUT FILTER
f
y
404
AI SUBROUTINES
e
407
DATA, TABLES, FILES & RECORDS
408
405
400

FIG. 6

FIG. 7


701
INSTITUTION ACTIVATES THE PERSONAL COMPUTER TO ACCESS INFORMATION MANAGEMENT SYSTEM
702
PERSONAL COMPUTER ESTABLISHES A COMMUNICATION CONNECTION TO THE WEB SITE ROUTER
703
INFORMATION MANAGEMENT SYSTEM FORWARDS RECEIVED QUERY AND DATA TO THE DATABASE SYSTEM
704
DATABASE SYSTEM ACTIVATES THE ACCESS CODE RECOGNITION PROCESS
ACCESS AUTHORIZED ?
NO
EXIT
YES
705
INITIAL OUTPUT FILTER DETERMINES THE NATURE OF THE QUERY AND APPROVES GENERATION OF STATISTICAL SUMMARY TO INSTITUTION
706
INITIAL OUTPUT FILTER TRANSMITS QUERY TO AI PATTERN RECOGNITION SUBROUTINES
707
AI PATTERN RECOGNITION SUBROUTINES COMPARE QUERY WITH DATA RESIDENT IN DATA TABLES, FILES AND RECORDS
708
AI PATTERN RECOGNITION SUBROUTINES TRANSMITS COMPARISON INFORMATION TO INSTITUTION QUERY OUTPUT FILTER
709
INSTITUTION QUERY OUTPUT FILTER PRODUCES A REPORT FOR INSTITUTION
710
INSTITUTION QUERY OUTPUT FILTER TRANSMITS THIS FINAL REPORT TO WEB SITE ROUTER
711
WEB SITE ROUTER FORWARDS REPORT TO INSTITUTION